UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

June 2023 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

DAREN LI,
aka "Devon,"
aka "KG-PERFECT,"
aka "RF," and
YICHENG ZHANG,
aka "Eason,"

Defendants.

CR No. 2:24-cr-00311-SVW

I N D I C T M E N T

[18 U.S.C. § 1956(h): Conspiracy to Commit Money Laundering; 18 U.S.C. § 1956(a)(2)(B)(i): International Money Laundering; 18 U.S.C. § 982: Criminal Forfeiture]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

At times relevant to this Indictment:

A. Defendants

1. Defendant DAREN LI ("LI"), also known as ("aka") "Devon," aka "KG-PERFECT," aka "RF," was a citizen of the People's Republic of China and Saint Christopher (St. Kitts) and Nevis, and resided at various times in the People's Republic of China, the Kingdom of Cambodia, and the United Arab Emirates.

2. Defendant YICHENG ZHANG ("ZHANG"), aka "Eason," was a

citizen of the People's Republic of China and resided in Los Angeles, California.

B. Co-Conspirators

3. Co-Conspirator 1 was a citizen of China and resided in multiple locations in the United States, including in Los Angeles, California; New York, New York; and Miami, Florida.

4. Co-Conspirator 2 was a citizen of the United States and resided in Los Angeles, California.

C. Foreign Entities and Bahamian Bank Accounts

5. GTAL (Cambodia) Co., Ltd. ("GTAL") was an entity incorporated under the laws of the Kingdom of Cambodia on or about September 10, 2019.

6. "Bahamas Account" #1 was an account at Deltec Bank & Trust ("Deltec Bank") in the Bahamas, opened by GTAL on or about August 9, 2021.

7. Axis Digital Limited ("Axis Digital") was an entity incorporated under the laws of the Commonwealth of the Bahamas on or about November 30, 2021.

8. "Bahamas Account #2" was an account at Deltec Bank in the Bahamas, opened by Axis Digital on or about February 25, 2022.

D. U.S. Shell Companies

9. B&C Commerce LLC ("B&C Commerce") was a shell company registered with the California Secretary of State on or about January 21, 2022, with a principal address in San Gabriel, California.

10. Jimei Trading Inc. ("Jimei Trading") was a shell company registered with the California Secretary of State on or about May 15, 2022, with a principal address in San Gabriel, California.

11. YXJ Trading Corporation ("YXJ Trading") was a shell company

registered with the California Secretary of State on or about July 30, 2022, with a principal address in Monterey Park, California.

12. SMX Beauty Inc. ("SMX Beauty") was a shell company registered with the California Secretary of State on or about October 13, 2022, with a principal address in Monterey Park, California.

13. SMX Travel Inc. ("SMX Travel") was a shell company registered with the California Secretary of State on or about October 13, 2022, with a principal address in Monterey Park, California.

E. Virtual-Currency Wallet

14. The virtual-currency wallet address beginning with TRteo (the "TRteo Address") was a wallet that received transfers of virtual currency converted from funds in Bahamas Account #1, Bahamas Account #2, and other sources. This wallet received approximately $341 million in virtual currency between April 2021 and the date of this indictment.

F. Definitions

15. "Digital currency" or "virtual currency" is currency that exists only in digital form; it has some of the characteristics of traditional money, but it does not have a physical equivalent. Cryptocurrency, a type of virtual currency, is a network-based medium of value or exchange that may be used as a substitute for traditional currency to buy goods or services, or exchanged for traditional currency or other cryptocurrencies. USDT, or Tether, is a virtual currency whose value is pegged to the U.S. dollar.

16. The term "spoofed" refers to domain spoofing, a process by which cybercriminals seek to persuade victims that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a fraudulent site controlled by a

cybercriminal.

17. In "pig butchering" fraud schemes (a term derived from a foreign-language phrase used to describe these crimes), scammers encounter victims on dating services, social media, or through unsolicited messages or calls, often masquerading as a wrong number. Scammers initiate relationships with victims and slowly gain their trust, eventually introducing the idea of making a business investment using cryptocurrency. Victims are then directed to other members of the scheme operating fraudulent cryptocurrency investment platforms and applications, where victims are persuaded to make financial investments. Once funds are sent to scammer-controlled accounts, the investment platform often falsely shows significant gains on the purported investment, and the victims are thus induced to make additional investments. Ultimately, the victims are unable to withdraw or recover their money, often resulting in significant losses for the victims.

18. In "customer service" or "tech support" fraud schemes, victims are contacted by fake customer service or technology support representatives. Scammers often pretend to represent a prominent company and contact the victim to alert them to a supposed infection with a computer virus or false issue with the victim's computer or other digital device. Scammers then take a variety of actions to defraud the victim, including, but not limited to, the following: (a) causing the victim to provide them with remote access to the victim's digital devices to supposedly remediate the problem, (b) requesting that funds be transferred to pay for assistance, and (c) advising the victim to transfer money from accounts that are supposedly compromised by the problem to accounts controlled by the scammer.

COUNT ONE

[18 U.S.C. § 1956(h)]

[DEFENDANTS LI AND ZHANG]

19. The Grand Jury hereby realleges and incorporates by reference paragraphs 1 through 18 of this Indictment here.

A. OBJECTS OF THE CONSPIRACY

20. Beginning on an unknown date, but no later than in or about August 2021, and continuing to on or about April 12, 2024, in Los Angeles County, within the Central District of California, and elsewhere, defendants LI and ZHANG, together with others known and unknown to the Grand Jury, knowingly conspired and agreed:

a. to conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, which, in fact, involved the proceeds of a specified unlawful activity, that is, wire fraud, committed in violation of Title 18, United States Code, Section 1343, and knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and

b. to transport, transmit, and transfer, and attempt to transport, transmit, and transfer, monetary instruments and funds from a place in the United States to and through a place outside of the United States, knowing that the monetary instruments and funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity, and which monetary instruments and funds were, in fact, the proceeds of a

specified unlawful activity, that is, wire fraud, committed in violation of Title 18, United States Code, Section 1343, and knowing that the transportation, transmission, and transfer was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds, in violation of Title 18, United States Code, Section 1956(a)(2)(B)(i).

B. THE MANNER AND MEANS OF THE CONSPIRACY

21. The objects of the conspiracy were to be accomplished in substance as follows:

Solicitation of Investment Fraud Victims

a. Unindicted co-conspirators would contact victims directly through unsolicited social-media interactions, telephone calls and messages, and online dating services.

b. Unindicted co-conspirators would gain the trust of victims by establishing either professional or romantic relationships with the victims. Unindicted co-conspirators would build these relationships through interstate communications, including, but not limited to, electronic messages sent via end-to-end encrypted applications.

c. Unindicted co-conspirators would promote fraudulent cryptocurrency investments to the victims after gaining the victims' trust.

d. Unindicted co-conspirators would establish spoofed domains and websites that resembled legitimate cryptocurrency trading platforms.

e. In some executions of the scheme, unindicted co-conspirators would fraudulently induce victims into investing in cryptocurrency through these fraudulent and spoofed investment

platforms.

f. In other executions of the scheme, unindicted co-conspirators would fraudulently induce victims into investing in cryptocurrency by sending funds via wire transfer.

g. Unindicted co-conspirators would fraudulently represent to victims that the victims' investments were appreciating when, in fact, those funds had been converted by members of the fraud scheme.

Solicitation of Customer Service and Tech Support Fraud Victims

h. Unindicted co-conspirators would fraudulently represent to victims through interstate communications, including, but not limited to, electronic messages and phone calls, that they were from a customer service or technology support company.

i. Unindicted co-conspirators would fraudulently induce victims to send funds via wire transfer or cryptocurrency trading platforms to purportedly remediate a non-existent virus or other false computer-related problem.

Receipt and Disposition of Fraud Proceeds

j. Co-conspirators would register dozens of shell companies with the California Secretary of State and elsewhere, including B&C Commerce, Jimei Trading, YXJ Trading, SMX Beauty, and SMX Travel.

k. Defendants LI and ZHANG would instruct co-conspirators, including Co-Conspirator 1, to open bank accounts in the names of various shell companies.

l. Co-conspirators, including Co-Conspirator 1, would receive victim funds in bank accounts established on behalf of shell companies and cause the further transfer of victim funds to domestic

and international bank accounts.

m. Defendants LI and ZHANG, and other co-conspirators, would monitor the receipt and execution of interstate and international wire transfers of victim funds, including to Bahamas Account #1 and Bahamas Account #2.

n. Defendants LI and ZHANG, and other co-conspirators, would cause wire transfers to be sent through various intermediary bank accounts before reaching their final beneficiary.

o. Defendant LI would possess corporate documents associated with shell companies that other co-conspirators would use to open bank accounts and funnel victim proceeds.

p. Defendants LI and ZHANG would receive victim funds in financial accounts they directly controlled.

q. Defendant LI would monitor the conversion of victim funds to USDT and the subsequent distribution of virtual currency to cryptocurrency wallets.

r. Defendants LI and ZHANG, and other co-conspirators, would communicate with each other and coordinate acts in furtherance of the conspiracy through multiple encrypted messaging services.

s. The fraud scheme involved more than $73.6 million in funds deposited into Bahamas Account #1 and Bahamas Account #2, including at least $59.8 million from U.S. shell companies that laundered victim proceeds.

t. After the funds were transferred into Bahamas Account #1 and Bahamas Account #2, Defendant LI and other co-conspirators, including Co-Conspirator 2, would direct the conversion of nearly all of the funds into USDT.

u. Defendant LI and other co-conspirators would provide

the virtual-currency wallet address (the TRteo Address) to Deltec Bank and others to receive the USDT.

v. Defendant LI and other co-conspirators would cause the transfer of USDT to the TRteo Address from Delchain Limited, a virtual-currency entity associated with Deltec Bank.

C. OVERT ACTS

22. In furtherance of the conspiracy and to accomplish its objects, defendants LI and ZHANG, Co-Conspirators 1 and 2, and others known and unknown to the Grand Jury, on or about the dates set forth below, committed and caused to be committed various overt acts, in the Central District of California and elsewhere, including, but not limited to, the following:

Overt Act No. 1: On April 11, 2022, defendant LI sent a message on a chat application soliciting a participant in the scheme.

Overt Act No. 2: On May 12, 2022, defendant ZHANG received $5,000 in his personal checking account directly from a victim of a pig-butchering scam.

Overt Act No. 3: On May 27, 2022, defendant LI sent messages on a chat application instructing an unindicted co-conspirator to open bank accounts at JPMorgan Chase and Wells Fargo for the shell company Jimei Trading.

Overt Act No. 4: On June 3, 2022, defendant LI sent messages on a chat application instructing an unindicted co-conspirator to open another bank account for the shell company Jimei Trading.

Overt Act No. 5: On June 8, 2022, defendant LI transferred approximately $999,383 in virtual currency from his personal cryptocurrency wallet to Co-Conspirator 2 to facilitate the operation of Bahamas Account #2.

Overt Act No. 6: Between June 24, 2022, and September 8, 2022, defendant LI or a co-conspirator caused approximately $713,100 to be sent in multiple transactions from Jimei Trading bank accounts to Bahamas Account #1 and Bahamas Account #2.

Overt Act No. 7: Between June 28, 2022, and July 11, 2022, defendant LI or a co-conspirator caused approximately $380,925 to be sent in multiple transactions from a B&C Commerce bank account to Bahamas Account #1 and Bahamas Account #2.

Overt Act No. 8: On July 15, 2022, defendant LI received approximately 798,403 USDT in his personal cryptocurrency wallet, which included victim funds from a pig-butchering scam.

Overt Act No. 9: On July 23, 2022, defendant LI transferred approximately 1,649,999 USDT, which included victim funds from a pig-butchering scam, from his personal cryptocurrency wallet to the TRteo Address.

Overt Act No. 10: On August 5, 2022, defendant LI sent a message on a chat application confirming that funds from Bahamas Account #2 that were exchanged for USDT should thereafter be transferred to the TRteo Address.

Overt Act No. 11: On August 30, 2022, defendant LI sent a message on a chat application to Co-Conspirator 1 with wiring instructions for Bahamas Account #1.

Overt Act No. 12: Between September 14 and 30, 2022, defendant LI or a co-conspirator caused approximately $1,190,000 to be sent in multiple transactions from YXJ Trading bank accounts to Bahamas Account #1 and Bahamas Account #2.

Overt Act No. 13: On October 1, 2022, defendant LI sent a message on a chat application to an unindicted co-conspirator to

facilitate a transfer of funds into a bank account held by the shell company YXJ Trading.

Overt Act No. 14: On October 12, 2022, defendant LI sent messages on a chat application to Co-Conspirator 1 with a list of entities including several shell companies that funneled victim proceeds from pig-butchering scams to Bahamas Account #1 and Bahamas Account #2.

Overt Act No. 15: On October 19, 2022, defendant LI sent a message on a chat application to an unindicted co-conspirator with the California Secretary of State records for shell company B&C Commerce.

Overt Act No. 16: From October 26, 2022, to at least October 28, 2022, defendants LI and ZHANG, and other co-conspirators, sent messages on a chat application instructing a co-conspirator to open U.S. bank accounts in the name of the shell companies SMX Beauty and SMX Travel.

Overt Act No. 17: On November 10, 2022, defendant LI sent a message on a chat application to a co-conspirator discussing paying a salary or a commission for the money-laundering services, including a 1.5 percent commission rate, explaining that, if a bank account were worth $1,000,000, the co-conspirator would receive $15,000.

Overt Act No. 18: Between November 28, 2022, and December 22, 2022, defendant LI, defendant ZHANG, or a co-conspirator caused approximately $2,285,760 to be sent in multiple transactions from SMX Beauty and SMX Travel bank accounts to Bahamas Account #1 and Bahamas Account #2.

Overt Act No. 19: On August 4, 2023, defendant LI sent messages on a chat application to Co-Conspirator 1 warning Co-

Conspirator 1 about recent law-enforcement action seizing funds from a financial institution used in the scheme.

Overt Act No. 20: On October 25, 2023, defendant ZHANG instructed Co-Conspirator 1 to make a videorecording at and a phone call to a U.S. financial institution where victim proceeds were frozen.

COUNTS TWO THROUGH SEVEN

[18 U.S.C. §§ 1956(a)(2)(B)(i), 2(a), (b)]

23. The Grand Jury re-alleges and incorporates paragraphs 1 through 18 of this Indictment here.

24. On or about the dates set forth below, in Los Angeles County, within the Central District of California, and elsewhere, defendants LI and ZHANG, and others known and unknown to the Grand Jury, each aiding and abetting the other, knowingly transported, transmitted, transferred, and willfully caused to be transported, transmitted, and transferred, the monetary instruments and funds listed below from a place in the United States to and through a place outside the United States, knowing that the monetary instruments and funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity, and which monetary instruments and funds, in fact, were derived from specified unlawful activity, that is, wire fraud, committed in violation of Title 18, United States Code, Section 1343, and knowing that such transportation, transmission, and transfer was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of such proceeds:

COUNT	DATE	WIRE TRANSFER	DEFENDANT/S
TWO	July 11, 2022	Bank wire transfer of $130,000 from a Bank of America account ending in 9287 to Bahamas Account #2.	LI
THREE	September 8, 2022	Bank wire transfer of $100,000 from a Bank of America account ending in 9287 to Bahamas Account #1.	LI

FOUR	December 6, 2022	Bank wire transfer of $189,000 from a JP Morgan Chase account ending in 5527 to Bahamas Account #1.	LI and ZHANG
FIVE	December 12, 2022	Bank wire transfer of $141,000 from a Bank of America account ending in 0186 to Bahamas Account #1.	LI and ZHANG
SIX	December 12, 2022	Bank wire transfer of $270,000 from a JP Morgan Chase account ending in 9773 to Bahamas Account #2.	LI and ZHANG
SEVEN	December 15, 2022	Bank wire transfer of $225,000 from a Bank of America account ending in 2607 to Bahamas Account #1.	LI and ZHANG

FORFEITURE ALLEGATION

[18 U.S.C. § 982]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 982(a)(2), in the event of any defendant's conviction of the offenses set forth in any of the counts set forth in this Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

(a) All right, title and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), any defendant so convicted shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been

//

//

//

substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

A TRUE BILL

/s/

Foreperson

E. MARTIN ESTRADA
United States Attorney

CAMERON L. SCHROEDER
Assistant United States Attorney
Chief, National Security Division

KHALDOUN SHOBAKI
Assistant United States Attorney
Chief, Cyber & Intellectual Property Crimes Section

LAUREN RESTREPO
Assistant United States Attorney
Deputy Chief, Cyber & Intellectual Property Crimes Section

MAXWELL COLL
Assistant United States Attorney
National Cryptocurrency Enforcement Team
Computer Crime & Intellectual Property Section

NISHA CHANDRAN
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section

STEFANIE SCHWARTZ
Trial Attorney
National Cryptocurrency Enforcement Team
Computer Crime & Intellectual Property Section